SHARED SECRET AUTHENTICATION PROTOCOL FOR CLIENT AND SERVER IN INTERNET BANKING APPLICATIONS

Hasan Al-Saedy

Abstract

In this paper the authentication concepts, in internet banking, are demonstrated. The available internet security technologies are explained, the strength and limitation of these security technologies are highlighted, and an automatic protocol to improve the authentication flaw of the internet banking applications is explained. Also a numerical example to explain the protocol is demonstrated. Finally the strength and limitation of the suggested protocol is given.

Keywords: Internet Banking, shared secret protocols, internet security technologies

INTRODUCTION:

Internet banking and other internet applications suffer from the internet security problems. These problems are fake Web site attack (Al Saedy, 2004), packet sniffing, packet spoofing, and packet hijacking (Mathew, 2003). Many technologies are available for internet security in general and the internet banking in particular. These technologies are subject to one or more of the above mentioned security attacks. Fake Web site attack is based on the use of a fake Web site, given that the majority of the internet users are unaware of this type of attack. In this paper the main internet security technologies, namely the S-HTTP and SSL/TSL are briefly described, the security problems associated with the two technologies are explained, and a client/server authentication protocol is introduce the protocol is based on the used of shared secret protocol in general and the zero knowledge protocol in particular. The advantages and limitations of the protocol are critically discussed.

Available Security Technologies:

S-HHTP is an extension of HTTP that provides a variety of security enhancement over the internet. The protocol is designed to introduce a security solution to the internet sensitive applications; security includes signature, authentication, and encryption. Authentication lets clients ensure that they are communicating with the right server and lets server ensures that it communicates with the right authorized client. Authentication is performed by using digital certificates issued by certification third party. Encryption makes data transferred over the network unintelligible to intruders and eavesdroppers. Digital signatures provide two features: the data integrity and non repudiation, non repudiation is that the receiver of data can prove to a third party that the sender really sent the transaction (Adam, 1995).

SSL protocol, originally developed by Netscape, SSL has been internationally accepted on the World Wide Web for authenticated and encrypted communication between clients and servers. The Internet Engineering Task Force (IETF) standard, called Transport Layer Security (TLS) is based on SSL. It is published as an IETF Internet-Draft; the TLS Protocol Version 1.0 Netscape product will fully support TLS (http://developer.netscape.com).

High level protocols like Hyper Text Transport Protocol (HTTP) and Internet Messaging Access Protocol (IMAP) work on the top of Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP controls the transport and routing of the data over the global network. The SSL protocol works below the high-level protocol and above the TCP/IP. Among the features of the SSL is the server authentication. In this protocol Public Key Encryption, specifically RSA is used for clients and servers authentication. SSL also supports the use of encryption algorithm, like Data Encryption Standard (DES) to secure the data communications. Implementing of the SSL/TLS needs the availability of the Trusted Third Party. This is a trusted security organization, established by the government and works under the control of the national central bank. The function of the trusted third party is issuing certificate to server, and control of the authentication of the clients and servers. Using the SSL/TLS will not solve the problems of packet sniffing and IP spoofing, however using encryption with SSL/TLS makes the packet cryptanalysis very hard task, but possible. The SSL/TSL is integrated with the application layer and can be implemented easily with high degree of flexibility compared with SHTTP protocols.

Internet Security Problems:

In this article the security problem of internet banking is addressed, threats to security are reality; these threats are fake Web site, man in the middle, replay attacks, sniffing, spoofing and packet hijacking. The majority of these attacks are viable on both security protocols (SHHP and SSL/TSL). The fake Web site that have been demonstrated in (Al Saedy, 2004) is the most easy to implement and is a highly effective attack. Using the shared secret protocol and namely the zero knowledge protocol will greatly enhance the security of internet banking. The reason for this is that no password sending or receiving in server/client communications, and accordingly no cryptanalysis is there. On the top of that the protocol eliminates the possibility of using the fake Web site attack.

Shared Secret Protocols:

In the proposed shared secret protocol for internet banking, it is assumed that the client has its secret and the server its own secret. Both client and server know the secret of each other. The first step the client interrogates the server, using zero knowledge, to make sure that the server knows its secret (the server secret). This is the identity proof of the server. If server proofs its identity to the client successfully, the second step is that the server interrogates the client to be sure from the identity of the client, again by using zero knowledge protocol. In case that the serve proofs its identity to the client and the client proofs its identity to the server, the connection is established and both server and client initiate sending/receiving packets, and finally they close the connection. In the next two sections both the theory and numerical example of shared secret protocol, namely the discrete logarithm are demonstrated. It is important to notice that neither the server nor the client revels secret.

Shared Secret Protocol: Discrete Logarithm:

Many zero knowledge protocols are available in cryptography (Schneier, 1995); in this article the discrete logarithm protocol is demonstrated. The protocol allows a person to prove his iden-

tity without using any token. The protocol uses the following variables and constants.

P is a prime number
x is a random number relatively prime to P – 1
A, B and P are public
x is kept secret and stands for PIN
A^x congruent B (mod P)

The protocol:

-The account owner generates t random numbers r1,r2, ..., rt, where all ri are less than P-1.

-The account owner computes hi = Ari mod P for all values of i , and sends them to the bank server via the ATM machine.

-The account owner and the bank server engage in a coin flipping protocol to generate t bits : b1,b2, ... , bt .

-For all t bits, the bank account owner does one of the following:
if bi = 0 he/she sends to the bank server ri
If bi = 1 he/she sends to the bank server si = (ri – rj) mod (P-1), where j is The lowest value for which bj = 1.

-For all t bits, the bank server confirms one of the following:
If bi = 0 that Ari congruent hi (mod P)
If bi = 1 that Asi congruent hihj-1 (mod P)

-The account owner sends to the bank server Z, where Z congruent (x – rj) Mod (P- 1).

-The bank server confirms that Az congruent Bhj-1 (mod P)
-The interceptor's probability of successfully cheating is 2-t

Numerical example:

Constants and variables:

Let P = 37, P-1 = 36, and x = 5;
x is relatively prime to 36;
A, B and P are public
A = 6, B = 6;
x is secret;
65 congruent 6(mod 37)

The protocol:
Account owner generates t random numbers less than 36;
Let t = 3 and the numbers 3, 4 and 5
3 < 36
4 < 36
5 < 36
Account owner computes h1, h2, and h3
h1 = 63 mod 37 = 261 mod 37 = 31
h2 = 64 mod 37 = 1566 mod 37 = 1
h3 = 65 mod 37 = 9396 mod 37 = 6
Account owner and the bank server engage in a coin flipping protocol to
Generate 3 bits;
b1 = 1;
b2 = 0;
b3 = 1;
Account owner sends to bank server
s1 = (r1 – r1) mod 36 = (3 – 3) mod 36 = 0
r2 = 4
s3 = (r3 –r1) mod 36 = (5 – 3) mod 36 = 2
The bank server confirms
60 = 31 * 31-1 mod 37 = 31 * 6 mod 37 = 1
64 = 1 mod 37
62 = 6* 31-1 mod 37 = 6 * 6 mod 37 = 36
Account owner sends to the bank server Z , where
Z = (5 – 3) mod 36 = 2
Bank server confirms that
62 = 6 * 31-1 mod 37 = 6*6 mod 37 = 36

Discussion and Conclusions:

In this paper the authentication problem of both client and server in internet banking is studied. The available security technologies are also demonstrated. The strength and limitation of these technologies are also discussed. Fake Web site attack is a potential risk and the tools and means to implement this risk are available. Also this sort of attack can easily be implemented by average computer user. Adding to the above the unawareness of the average users of the internet banking system. In this paper the concepts of the shared secret protocol is introducing. The protocol runs automatically to authenticate both client and server and give a warning in case of discovering any security violation. The advantage of the protocol is that neither the server nor the client revel any information to intruders, also the computer time required to do the protocol process is insignificant.

Reference:

(1) Al-Saedy Hasan, Internet banking: Server authentication is a must, 3rd International Business Information Management Conference (3rd IBIMA) on December 14, 15, and 16, 2004, Cozumel, Mexico

(2) Tanase Mathew, IP Spoofing: An introduction, March 11, 2003, http://www.securityfocus.com/infocus/1674

(3) Shostack Adam, An overview of SHHP, May 1995, http://www.homeport.org/~adam/shttp.html

(4) Introduction to SSL, http://developer.netscape.com/docs/manuals/security/sslin/contents.htm

(5) Schneier Bruce, Applied Cryptography: Protocols, Algorithms, and Source code in C, Second Edition, Wiley, 1995.

Dr. Hasan Al-Saedy
Associate Professor
Skyline College
Sharjah , UAE
Tel.: 00971 6 5439444
e-mail: hasan@skylincollege.info